



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,996	08/31/2001	Brian K. Martin	RSW920010151US1	1846

46320 7590 10/07/2005

CHRISTOPHER & WEISBERG, PA
200 E. LAS OLAS BLVD
SUITE 2040
FT LAUDERDALE, FL 33301

EXAMINER

HA, LEYNNA A

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 10/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/944,996

Applicant(s)

MARTIN, BRIAN K.

Examiner

LEYNNA T. HA

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 June 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 8/31/01.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-13 have been re-examined and are pending.
2. This is a Final rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. **Claim 1 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.**

Claim 1 on lines 10-12 was amended wherein contains new subject matter "when said state machine in said restricting state". According to the specification, only mentions ignore access requests (pg.11, line 11; pg.12, line19 – pg.13, line 1), but fails to further include when the state machine is in restricting state.

Response to Arguments

4. Applicant's arguments filed June 16, 2005 have been fully considered but they are not persuasive.

In regards to claims 1, 8-9, and 12-13:

The argument made regarding Reid teaching a single request and failing to disclose applicant's plurality of requests is traverse. The claim language broadly states that there are multiple requests for access which could be a connection from an external network to a protect second network. The claimed invention does not include having multiple requests for multiple connections. Thus, the plurality of requests as disclosed by Reid are users or users of different groups or data packets entering attempting to a connection to the second network (col.4, lines 3-5 and 54-65; col.5, lines 5-22; col.6, lines 4-5; co.7, lines 16-19; col.12, lines 51-55; FIG.2; and FIG.3). By Reid discussing initiating the connection request does not mean there is a single request but means requesting to a single connection from either the user or groups (col.6, lines 4-5). Reid further discloses a plurality of requests where the firewall apply rules to the network in which data packets are entering (col.4, lines 3-5) and for each connection attempt the firewall receives and processes from these the users/groups request attempts or packets to the ACLs for the connection (col.5, lines 51-53). The claim language states plurality of requests where Reid reads on having many

Art Unit: 2135

users/groups or packets requesting access (i.e. connection) from the network device to the protected network. Innuendo, the claimed invention meant to include plurality of requests is multiple access (connections), Reid does disclose anonymous FTP connections and VPN connections (col.8, lines 2-3 and 47-50) and connection counts for a connection (col.14, lines 45-46).

Although the examiner may point to one or two citations in the last rejection, the rejection is not only limited to what was cited but that the entire reference (Reid, et al.) should provide more details and explanations to the rejected claims.

In reply to claims 7 and 11:

The examiner traverses the argument where Reid does not have a second request in addition to a first request that transitions to a final state. By Reid showing the description of each value that is determined by the ACL of the firewall for each connection is the one of two access requests. Reid discloses making two calls to the ACLs where a call is a request. The first call identifies access parameter where the values is the transitioning criteria to transition to the intermediate state (col.12, line 66 – col.14, line 37). The second call is the final state transition (col.14, lines 43-47).

In regards to the argument of not responding to the request:

no response or ignores to requests in the restricting state is where Reid discloses the connection is not allowed therefore need not make any further calls for that connection. Further, Reid discusses only to

Art Unit: 2135

respond to the incoming packet which is the request if the region table indicates that the ping is enabled. Thus, it is inherent to not respond to the packet if the region table indicates the ping is disabled. (col.15, lines 11-13 and 61-63)

In reply to claim 10:

The examiner traverses the argument that Rothermel does not have comparison of hash result to hash password in addition to a timestamp. Rothermel discloses that the NSDs and supervisor devices provide information only to authorized devices or users such as the hashing passwords (col.5, lines 62-64) where hash password is information that is used for security related process that involves comparison process. Thus, when Rothermel indicates that time stamp is one of the security information it is part of the security policy of the particular packet (col.11, line 63 – col.12, line 6) along with the hash password information that will be used in the comparison process (col.6, lines 58-64).

5. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., information contained in prior connection request) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Art Unit: 2135

In reply to claim 1:

The argument where applicant indicates that Reid discloses the condition for responding is in the current connection request and that it should be in a prior connection request. However, claim language does not cite a prior connection request.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-9 and 11-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Reid, et al. (US 6,182,226).

As per claim 1:

Reid discloses a stealth firewall comprising:

Art Unit: 2135

a first network interface to an external network; **(col.2, lines 66-67)**

a second network interface to an internal network; **(col.3, lines 55-58)**

a packet filter for restricting access to said internal network **(col.3, lines 61-63)**; and,

a state machine pre-configured to transition across a plurality of internal states, from a restricting state to an access state **(col.5, line 58-col.6, line 40)**, conditioned upon receiving a plurality of requests to access said internal network, said plurality of requests collectively comprising a code for causing said state machine to transition from said restricting state to said access state which causes said packet filter to permit access to said internal network; wherein **[the plurality of requests as disclosed by Reid are users or users of different groups or data packets entering attempting to a connection to the second network (col.4, lines 3-5 and 54-65; col.5, lines 5-22; col.6, lines 4-5; co.7, lines 16-19; col.12, lines 51-55; FIG.2; and FIG.3)]**

said packet filter not responding to said external network upon receiving any requests from said external network to access said internal network when said state machine in said restricting state. **[no response or ignores to requests in the restricting state is where Reid discloses the connection is not allowed therefore need not make any further calls for that connection. (col.15, lines 11-13 and 61-63)]**

Art Unit: 2135

As per claim 2: See col.1, lines 35-48 and col.4, line 20; discussing requests from said external network comprise transport control protocol (TCP) SYN messages.

As per claim 3: See col.1, lines 35-48 and col.4, line 20; discussing each state in said state machine corresponds to data in a specified field of said TCP SYN messages.

As per claim 4: See col.6, lines 12-13 and col.7, lines 40-43; discussing specified field comprises a destination port field.

As per claim 5: See col.5, lines 54-55; discussing code is a rolling code which can vary according to time.

As per claim 6: See col.6, lines 9-13; discussing packet filter can permit access to a specific port in said internal network based upon a destination port specified in a TCP SYN message received after transitioning to said access state in said state machine.

As per claim 7:

Reid discloses a method for permitting access to a network protected behind a stealth firewall comprising the steps of:

initializing a state machine configured to grant access to the stealth firewall (**col.5, lines 35-53**) contingent upon said state machine transitioning across a plurality of internal states responsive to receiving a plurality of requests to access the network from a single network device, said plurality of requests collectively comprising a code for causing said state machine to permit access to the network; **[the plurality of**

Art Unit: 2135

requests as disclosed by Reid are users or users of different groups or data packets entering attempting to a connection to the second network (col.4, lines 3-5 and 54-65; col.5, lines 5-22; col.6, lines 4-5; co.7, lines 16-19; col.12, lines 51-55; FIG.2; and FIG.3)]

receiving an access request from a network device in a network which is external to the network protected behind the stealth firewall, identifying an access parameter in said access request **(col.7, lines 31-51)** and transitioning from an initial state in said state machine to an intermediate state if said identified access request satisfies transitioning criteria associated with said state machine for transitioning from said initial state to said intermediate state; **(col.5, line 58-col.6, line 40)**

receiving a further access request from said network device in said network which is external to the network protected behind the stealth firewall, identifying a further access parameter in said further access request and transitioning from an intermediate state in said state machine to a final state if said identified further access request satisfies transitioning criteria associated with said state machine for transitioning from an intermediate state to said final state; **(col.13, lines 31-67)**

not providing a response to said network device upon receiving each said access request from said network device in said network which is external to the network protected behind the stealth firewall unless said network device provides a sequence of access requests to the stealth firewall causing said state machine to transition to said final state; and,

Art Unit: 2135

[no response or ignores to requests in the restricting state is where Reid discloses the connection is not allowed therefore need not make any further calls for that connection. (col.15, lines 11-13 and 61-63)]

upon transitioning to said final state, permitting said network device to access the network protected behind the stealth firewall.

(col.16, lines 59-66)

As per claim 8:

Reid discloses a method for permitting access to a network protected behind a stealth firewall comprising the steps of:

receiving a plurality of access requests from a plurality of network devices **[the plurality of requests as disclosed by Reid are users or users of different groups or data packets entering attempting to a connection to the second network (col.4, lines 3-5 and 54-65; col.5, lines 5-22; col.6, lines 4-5; co.7, lines 16-19; col.12, lines 51-55; FIG.2; and FIG.3)]** which are external to the network protected behind the stealth firewall; **(col.3, lines 34-35)**

not providing a response to said plurality of network device upon receiving each of said access requests; **[no response or ignores to requests in the restricting state is where Reid discloses the connection is not allowed therefore need not make any further calls for that connection. (col.15, lines 11-13 and 61-63)]**

Art Unit: 2135

identifying access request parameters in said received access requests; **(col.5, lines 58-63)**

performing state transitions in a state machine in the stealth firewall based upon identifying particular ones of said identified access request parameters; and, **(col.7, lines 34-51)**

upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters. **(col.16, lines 20-65)**

As per claim 9:

Reid discloses a method for permitting access to a network protected behind a stealth firewall comprising the steps of:

configuring a state machine to grant access to the stealth firewall contingent upon said state machine transitioning through a plurality of states **(col.16, lines 20-65)** based upon a sequence of access request parameters identified in received access requests from a single network device; **[the plurality of requests as disclosed by Reid are users or users of different groups or data packets entering attempting to a connection to the second network (col.4, lines 3-5 and 54-65; col.5, lines 5-22; col.6, lines 4-5; co.7, lines 16-19; col.12, lines 51-55; FIG.2; and FIG.3)]**

setting said sequence of access parameters to a specific set of access parameters; and, **(col.7, lines 34-51)**

disposing said state machine in the stealth firewall. **(col.5, lines 34-38)**

As per claim 11:

Reid discloses a machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

initializing a state machine configured to grant access to the stealth firewall **(col.5, lines 35-53)** contingent upon said state machine transitioning across a plurality of internal states responsive to receiving a plurality of requests to access the network from a single network device, said plurality of requests collectively comprising a code for causing said state machine to permit access to the network; **[the plurality of requests as disclosed by Reid are users or users of different groups or data packets entering attempting to a connection to the second network (col.4, lines 3-5 and 54-65; col.5, lines 5-22; col.6, lines 4-5; co.7, lines 16-19; col.12, lines 51-55; FIG.2; and FIG.3)]**

receiving an access request from a network device in a network which is external to the network protected behind the stealth firewall, identifying an access parameter in said access request **(col.7, lines 31-51)** and transitioning from an initial state in said state machine to an

Art Unit: 2135

intermediate state if said identified access request satisfies transitioning criteria associated with said state machine for transitioning from said initial state to said intermediate state; **(col.5, line 58-col.6, line 40)**

receiving a further access request from said network device in said network which is external to the network protected behind the stealth firewall, identifying a further access parameter in said further access request and transitioning from an intermediate state in said state machine to a final state if said identified further access request satisfies transitioning criteria associated with said state machine for transitioning from an intermediate state to said final state; **(col.13, lines 31-67)**

not providing a response to said network device upon receiving each said access request from said network device in said network which is external to the network protected behind the stealth firewall unless said network device provides a sequence of access requests to the stealth firewall causing said state machine to transition to said final state; and, **[no response or ignores to requests in the restricting state is where Reid discloses the connection is not allowed therefore need not make any further calls for that connection. (col.15, lines 11-13 and 61-63)]**

upon transitioning to said final state, permitting said network device to access the network protected behind the stealth firewall. **(col.16, lines 59-66)**

Art Unit: 2135

As per claim 12:

Reid discloses a machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

receiving a plurality of access requests **[the plurality of requests as disclosed by Reid are users or users of different groups or data packets entering attempting to a connection to the second network (col.4, lines 3-5 and 54-65; col.5, lines 5-22; col.6, lines 4-5; co.7, lines 16-19; col.12, lines 51-55; FIG.2; and FIG.3)]** from a plurality of network devices which are external to the network protected behind the stealth firewall; **(col.3, lines 34-35)**

not providing a response to said plurality of network device upon receiving each of said access requests; **[no response or ignores to requests in the restricting state is where Reid discloses the connection is not allowed therefore need not make any further calls for that connection. (col.15, lines 11-13 and 61-63)]**

identifying access request parameters in said received access requests; **(col.5, lines 58-63)**

performing state transitions in a state machine in the stealth firewall based upon identifying particular ones of said identified access request parameters; and, **(col.7, lines 34-51)**

upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters. **(col.16, lines 20-65)**

As per claim 13:

Reid discloses a machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

configuring a state machine to grant access to the stealth firewall **(col.16, lines 20-65)** contingent upon said state machine transitioning through a plurality of states based upon a sequence of access request parameters identified in received access requests from a single network device; **[the plurality of requests as disclosed by Reid are users or users of different groups or data packets entering attempting to a connection to the second network (col.4, lines 3-5 and 54-65; col.5, lines 5-22; col.6, lines 4-5; co.7, lines 16-19; col.12, lines 51-55; FIG.2; and FIG.3)]**

setting said sequence of access parameters to a specific set of access parameters; and, **(col.7, lines 34-51)**

Art Unit: 2135

disposing said state machine in the stealth firewall. (**col.5, lines 34-38**)

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claim 10 is rejected under 35 U.S.C. 102(e) as being anticipated by Rothermal, et al. (US 6,678,827).

As per claim 10:

Rothermal discloses a stealth firewall comprising:

a first network interface to an external network; a second network interface to an internal network; (**col.1, lines 23-35**)

a packet filter for restricting access to said internal network (**col.4, lines 51-54**), said packet filter ignoring requests from said external network to access said internal network; (**col.5, lines 14-17**)

Art Unit: 2135

fixed storage in which at least one authentication password can be stored; **(col.6, lines 60-62)**

a hash processor configured to apply a hashing algorithm to said stored at least one authentication password; and, **(col.5, lines 63-64)**

a comparator configured to compare a hashed password and timestamp received from said first network interface **(col.6, lines 36-49)**, with a hashed result produced by said hash processor for a stored password associated with a user at said first network interface **(col.12, lines 5-6 and col.13, lines 47-67)**, said comparator causing said packet filter to permit access to said internal network where said hashed password and timestamp matches said hashed result.

[Rothermel discloses that the NSDs and supervisor devices provide information only to authorized devices or users such as the hashing passwords (col.5, lines 62-64) where hash password is information that is used for security related process that involves comparison process. Thus, when Rothermel indicates that time stamp is one of the security information it is part of the security policy of the particular packet (col.11, line 63 – col.12, line 6) along with the hash password information that will be used in the comparison process (col.6, lines 58-64).]

Conclusion

8. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

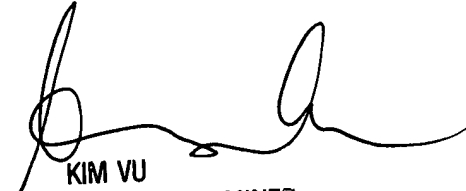
Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Lha



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100